UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/642,878	08/18/2003	Jagdeep Singh Sahota	P-15100US (930676.00150)	3312

65357 7590 10/03/2008

Quarles & Brady LLP
TWO NORTH CENTRAL AVENUE
One Renaissance Square
PHOENIX, AZ 85004-2391

EXAMINER	
SHUMATE, PAUL W	

ART UNIT	PAPER NUMBER
3693	

MAIL DATE	DELIVERY MODE
10/03/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/642,878	SAHOTA ET AL.	
	Examiner	Art Unit	
	PAUL SHUMATE	3693	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 May 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *14-21 and 26-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *14-21 and 26-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *26 February 2008*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Status of Claims

1. This action is in reply to the communication filed on 04/12/2008.

2. Claims 14 and 28 have been amended by Applicant.

3. Claims 22-25 and 29-49 are cancelled by Applicant.

4. Claims 1-13 were previously cancelled by Applicant.

5. Claims 14-21 and 26-28 are currently pending and have been examined.

Claim Objections

6. Previously cited objections are moot due to the cancellation of the relevant claims and have therefore been removed.

Claim Rejections - 35 USC § 112

7. Previously cited rejection regarding claim 26 has been removed in response to Applicant's amendment.

8. Previously cited rejections regarding claims 39-41, 43-45, 47 and 48 are moot due to the cancellation of the relevant claims and have therefore been removed.

Claim Rejections - 35 USC § 101

9. Previously cited rejections regarding claims 39-41, 43-45, 47 and 48 are moot due to the cancellation of the relevant claims and have therefore been removed.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claim(s) 14-19, 27, and 28 rejected under 35 U.S.C. 103(a) as being unpatentable over Li, US PGPub No.: 2002/0153424, in view of Buer, US Patent No.: 5,835,599, further in view of McGregor et al., US PGPub No.: 2002/0180584.

As per claim 14, Li teaches a processor-implemented method of dynamically creating a verification value for a transaction (see at least paragraph(s) 0007) comprising: creating, in response to the transaction involving a payment device, a base record having a first data value and a second data value (see at least paragraph(s) 0009). Li teaches that the creation of the dynamic digital certificate (verification value) is a function of a first group of variables and a second group of variables. The first group comprises the internally stored credit card account number, the card issuing date and time, and the card expiration date. The second group comprises dynamic data such as the instant date and time at which the transaction is taking place (see at least paragraph(s) 0009, 0024).

While Li does teach a symmetric encryption authentication method and system (see at least paragraph(s) 0007, 0012, 0020) that runs an encryption algorithm on plaintext data, which is formed from both the internally stored and the dynamic data, to produce a dynamic digital certificate that is compared against an independently created authentication code created by the authentication system, Li does not explicitly disclose the encryption steps of: splitting the base record into a first field and a second field; encrypting the first field using a first encryption key; performing an exclusive-OR (XOR) operation on the encrypted first field and the second field to produce a first result; encrypting the first result using a second encryption key to produce a second result; decrypting the second result using a decryption key to

produce a third result; encrypting the third result using a third encryption key to produce a fourth result; sequentially extracting each value between 0 and 9 from the most-significant digit to the least-significant digit of the fourth result to produce a fifth result; sequentially extracting and subtracting hexadecimal A from each value between hexadecimal A and hexadecimal F from the most-significant digit to the least-significant digit of the fourth result to produce the sixth result; concatenating the fifth result and the sixth result to produce a seventh result; selecting one or more values from the seventh result as a verification value for the transaction.

Buer, however, teaches splitting plaintext into 64-bit blocks P1 and P2 (see at least column 1 lines 57-59, column 2 lines 7-8, column 4 lines 26-32, and column 5 lines 48-50) encrypting blocks with an encryption key (see at least column 4 lines 1-4 and column 4 lines 36-40) performing an XOR operation on an unencrypted (plaintext) block and on an encrypted (ciphertext) block (see at least column 4 lines 20-22, column 4 lines 46-48, and column 5 lines 7-10) and encrypting encrypted results iteratively blocks (see at least column 4 lines 36-40). Buer notes that his teachings contemplate using different combinations and numbers of cipher stages, feedback paths, and output taps (see at least column 3 lines 3-6). Buer further teaches that decryption can be done with the same principle architecture used for encryption (see at least column 5 lines 5-6 and column 6 lines 58-60) and that decryption is the act of returning encrypted data back into its original form (see at least column 1 lines 14-15). Because the method is still in the process of creating an encrypted verification value, and because a decryption step that doesn't result in a decrypted (original form) value is substantially the same as an encryption step, the step of decrypting the second result using a decryption key to produce a third result is interpreted to be equivalent to encrypting the second result using an encryption key to produce a third result, and is therefore taught by Buer in at least column 3 lines 3-6 and column 4 lines 36-40. Buer further teaches extracting, rearranging, and manipulating data blocks using substitutions in conjunction with permutations (see at least column 5 lines 45-47), expansion permutations (see at least column 5 lines 55-64), transformations, circular shifts, compression permutations (see at least column 6 lines 1-11), S-box substitutions, P-box permutations (see at least column 6 lines 17-32), and concatenation to produce a final encoded value (see at least column 4 lines 13-14).

It would have been obvious at the time the invention was made to a person having ordinary skill in the art to have incorporated the steps taught by Buer into the teachings of Li because all these steps are old and well known in the art and different combinations and numbers of cipher stages, feedback paths, and output tags are employed routinely in many different strategies and methods for data encryption depending on the desired ratio of security to encryption/decryption speed (see at least column 1 lines 32-35, column 2 lines 11-19, and column 3 lines 3-6).

Further, neither Li nor Buest explicitly teach using an application transaction counter value in the verification process or in generating a verification value. McGregor, however, teaches a system and method for increasing transaction security which includes the use of a transaction counter value in the generation of a security key used to authenticate a user and verify a transaction (see at least Figure 3 and paragraph(s) 0013, 0014, 0041, 0042). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to have incorporated a transaction counter value to be use in the generation of a security key (verification value) because this helps increase transaction security in a manner already compatible with the existing infrastructure which, inter alia, prevents a thief from using stolen account information, from a receipt or similar record listing important card account information, to make fraudulent online or telephonic transactions (see at least paragraph(s) 0010, 0011 in McGregor).

As per claims 15, 16, 17, 18, Buer further teaches using equivalent first, second, and third encryption keys (see at least column 1 lines 57-59, column 3 lines 13-14, column 3 lines 56-59, column 4 lines 1-2, and column 4 lines 36-40) using different encryption/decryption keys (see at least column 6 lines 11-13, column 7 lines 31-34, and column 8 lines 13-16) and that the base record is 128-bits in length (see at least column 4 lines 26-32).

As per claim 19 Li further teaches the first data value comprises: a primary account number for the payment service (see at least paragraph(s) 0008, 0009, 0020).

As per claim 27, Buer further teaches padding data to a predetermined length (see at least column 4 lines 8-11).

As per claim 28, Li teaches that the dynamic digital certificate is created by an encryption algorithm on the card. The certificate is a function of variables including both data stored on the card and current transaction data. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to base the encryption keys on data stored on the card because this minimizes the chance of fraud because it would be nearly impossible for anyone other than the card issuer or the card itself to replicate the encryption algorithm.

12. Claim(s) 20, 21, and 26 rejected under 35 U.S.C. 103(a) as being unpatentable over Li, in view of Buer, in view of McGregor et al., further in view of Official Notice.

As per claims 20, 21, and 26, the examiner takes Official Notice that the limitations added by these claims are old and well known in the art of digital transaction verification and encryption to use unique identification numbers known and accessible by both payment devices and their host systems in the process of generating verification values to be used in authenticating transactions. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to base an encrypted transaction verification value on unique identifier variables and/or other personalized variables which uniquely identify specific payment devices, service providers, types of payment services, and payment service expiration dates because these are all values which are readily accessible by payment devices and payment service providers but are not readily accessible to anyone else. Further, it could be argued that Li's teachings of using the credit card account number and the credit card issuance or expiration dates in generating a verification value actually do teach the limitations of claims 20, 21, and 26 since a credit card account number does uniquely identify the credit card itself, it identifies a unique service provider or payment service in the card account number's first six digits (4xxxxx for Visa, 51xxxx-55xxxx for MasterCard, etc), and it also indirectly identifies the actual bank or institution which issued the card account since a merchant is able to determine which bank or institution is responsible for transferring funds to them on a buyer's behalf strictly based on the card account number used in the relevant transaction.

Response to Arguments

13. Applicant argues that Li and Buer both fail to teach or suggest a transaction counter used to generate a verification value. The examiner agrees but this argument is moot in view of the new ground(s) of rejection. Further, Applicant requested a specific reference which teaches a transaction counter used to generate a verification value. As explained in the rejection of claim 14 as shown above, McGregor clearly teaches using a transaction counter in the generation of a security key used to verify and authenticate transactions.

14. **THIS ACTION IS MADE FINAL**. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul Shumate whose telephone number is 571-270-1830. The examiner can normally be reached on M-F 8:30 AM - 6:00 PM, EST alt Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Kramer can be reached on 571-272-6783. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Name: Paul W. Shumate
Title: Patent Examiner
Date: 09/15/08
Signature: /Paul Shumate/
Examiner, Art Unit 3693

/James A. Kramer/

Supervisory Patent Examiner, Art Unit 3693